УТВЕРЖДЕНО

АКСФ.501490.008 91

ПАК АУТЕНТИФИКАЦИ И БЕЗОПАСНОГО ХРАНЕНИЯ ИНФОРМАЦИИ «РУТОКЕН» V. 4

Руководство пользователя

АКСФ.501490.008 91

Листов 21

Инв.№подл.	Подп. и дата	Взам.инв.№	Инв.№дубл.	Подп. и дата

2021

Аннотация

Настоящий документ предназначен для пользователей, осуществляющих эксплуатацию программно-аппаратного комплекса «Рутокен» версии 4 (далее ПАК «Рутокен» v. 4). В настоящем документе приведены общие сведения, описание возможностей использования ПАК «Рутокен» v. 4, а также условия использования ПАК.

Содержание

1. Назначение программно-аппаратного комплекса 3
1.1 Функциональное назначение 3
1.2 Эксплуатационное назначение 3
1.3 Функции ПАК «Рутокен» v. 4 4
2. Условия функционирования ПАК 5
2.1 Минимальный состав аппаратных средств 5
2.2 Минимальный состав программных средств 6
3. Начало работы с ПАК «Рутокен» v. 4 7
3.1 Состав ПАК «Рутокен» v. 4 7
3.2 Начало работы с ПАК «Рутокен» v. 4 7
4. Описание функционирования 9
5. Аварийные ситуации 22

1. НАЗНАЧЕНИЕ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА

1.1 Функциональное назначение

ПАК «Рутокен» v. 4» предназначен для выполнения функций по защите информации, а именно: хранение ключевой и управление доступом к ключевой информации. Обеспечивает контроль доступа к компьютеру, поддержку любого числа пользователей (владельцев ПАК «Рутокен» v. 4) на одном компьютере, безопасное хранение в одном устройстве большого количества данных: файлов, ключей шифрования, цифровых сертификатов

1.2 Эксплуатационное назначение

ПАК «Рутокен» v. 4 может быть использован в приложениях, где прежде использовались пароли при доступе к БД, Web-серверам, VPN-сетям и security-ориентированным приложениям на программно-аппаратную аутентификацию, обеспечивает надежность и безопасность процесса аутентификации.

Электронные идентификаторы ПАК «Рутокен» v. 4 представляют собой комбинацию активного и пассивного устройств аутентификации, в зависимости от задачи. Они предоставляют вычислительную платформу, на которой информация может храниться и обрабатываться безопасно.

Информация, хранящаяся в памяти электронных идентификаторов, может быть организована таким образом, чтобы доступ к ней полностью контролировался его владельцем или поставщиком приложений

Ключи и PIN-коды хранятся в памяти электронного идентификатора в специальных объектах файловой системы, доступ к этим объектам имеет только сам электронный идентификатор.

1.3 Функции ПАК «Рутокен» v. 4

- Хранение паролей для доступа к системам, сетям и т.п.;
- Хранение ключей шифрование и ключей электронной подписи;
- Хранение ключей для целей аутентификации;
- Безопасное хранение информации;
- Управление доступом к информации и ключам, хранящимся на электронном идентификаторе.

2. УСЛОВИЯ ФУНКЦИОНИРОВАНИЯ ПАК

1. Оберегайте электронный идентификатор от механических воздействий (падения, сотрясения, вибрации и т. п.), от воздействия высоких и низких температур, агрессивных сред, высокого напряжения; все это может привести к его поломке.
2. Не прилагайте излишних усилий при подсоединении токена к порту компьютера, карты в карт-ридер.
3. Не допускайте попадания на электронный идентификатор (особенно на его разъем) пыли, грязи, влаги и т. п. При засорении разъема токена примите меры для их очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование органических растворителей недопустимо.
4. Не разбирайте электронный идентификатор! Кроме того, что при этом будет утрачена гарантия на идентификатор, такие действия могут привести к поломке корпуса, а также к порче или поломке элементов печатного монтажа и, как следствие - к ненадежной работе или выходу из строя самого устройства.
5. В случае неисправности или неправильного функционирования электронного идентификатора обращайтесь к фирме-разработчику прикладного ПО.

2.1 Минимальный состав аппаратных средств

Элемент	Параметр
Процессор	1 ГГц с архитектурой x86 для всех тридцатидвухразрядных версий ОС, указанных выше 1ГГц с архитектурой x64 для всех версий ОС, указанных выше, кроме ОС Microsoft Windows Server 2008 Standard/Enterprise/Datacenter/Web Server SP2

Элемент	Параметр
	(64-bit) и Microsoft Windows Server 2008 Standard/Enterprise/Datacenter/Web Server R2 (64-bit) 1,4 ГГц с архитектурой x64 для ОС Microsoft Windows Server 2008 Standard/Enterprise/Datacenter/Web Server SP2 (64-bit) и Microsoft Windows Server 2008 Standard/Enterprise/Datacenter/Web Server R2 (64-bit)
Оперативная память	512 МБ
Жесткий диск (свободное пространство)	20 МБ
Порт	Свободный USB-порт для установки устройства, входящего в состав ПАК «Рутокен» v. 4 / ридер смарт-карт/слот для карты micro SD

2.2 Минимальный состав программных средств

Элемент	Параметр
Операционная система	ОС Microsoft Windows 8.1 (32/64-bit), ОС Microsoft Windows 10 (32/64-bit), ОС Альт Сервер 8 (32/64-bit), ОС Альт Рабочая станция 8 (32/64-bit), ОС Альт Образование 8 (32/64-bit), ОС Альт Линукс СПТ 7 (32/64-bit), ОС Альт 8 СП (32/64-bit), EMIAS OS 1.0, ОС Astra Linux Special Edition (РУСБ.10015-01) (32/64-bit), ОС Astra Linux Common Edition (32/64-bit)

3. НАЧАЛО РАБОТЫ С ПАК «РУТОКЕН» V. 4

3.1 Состав ПАК «Рутокен» v. 4

В состав ПАК «Рутокен» v. 4 входит:

- электронный идентификатор Рутокен. Электронный идентификатор может быть представлен следующими моделями:
- Рутокен ЭЦП SC;
- Рутокен ЭЦП 2.0 2100;
- Рутокен ЭЦП 2.0;
- Рутокен ЭЦП 2.0 micro;
- Рутокен ЭЦП, PKI версия;
- Рутокен ЭЦП micro, PKI версия;
- Рутокен ЭЦП 2.0 Flash;
- Рутокен Lite SD;
- «Rutoken Lite» (Рутокен Lite);
- «Rutoken S» (Рутокен S).

3.2 Начало работы с ПАК «Рутокен» v. 4

1. Для работы с программным обеспечением ПАК «Рутокен» v. 4 необходимо файлы, входящие в состав программного обеспечения ПАК «Рутокен» v. 4 в одну директорию на ПЭВМ Пользователя. В случае работы с ОС Windows следует установить драйверы ПАК «Рутокен» v. 4 путем запуска исполняемого файла rtDrivers.exe.
2. При необходимости следует перезагрузит компьютер.
3. Подсоедините электронный идентификатор к свободному USB-порту или вставьте в карт-ридер.
4. Произведите установку прикладного ПО, следуя инструкции разработчиков.

3.3 Удаление программного обеспечения

Для удаления программного обеспечения с ОС Linux достаточно удалить содержимое директории ПЭВМ пользователя, в которую было перенесены дистрибутивы ПО ПАК «Рутокен» v. 4.

В случае удаления ПО с ОС Windows помимо удаления содержимого директории необходимо через апплет операционной системы **Установка и удаления программ** удалить Драйверы Рутокен.

4. ОПИСАНИЕ ФУНКЦИОНИРОВАНИЯ

4.1 Использование на ОС семейства Windows

4.1.1 Панель управления Рутокен

Утилита администрирования предназначена, в первую очередь, для использования администраторами систем безопасности или, иначе говоря, офицерами безопасности.

Утилита администрирования позволяет выполнять следующие операции:

- Получение информации о подключенных устройствах
- Разблокирование PIN-кода Пользователя
- Установка новых PIN-кодов Пользователя и Администратора
- Изменение символьного имени устройства
- Установление минимальной длины PIN-кодов Пользователя и Администратора
- Установление максимального числа последовательных попыток ввода PIN-кода Пользователя и администратора

4.1.1.1 Главное окно утилиты

Перед запуском **Панели управления Рутокен** убедитесь в том, что в системе установлено ПО из состава ПАК «Рутокен» v. 4. Если устройство не подключено, подсоедините его к свободному USB-порту/вставьте в карт-ридер/слот microSD.

Главное окно содержит элементы управления основными функциями. Неактивные элементы будут недоступны до выполнения операции Login и ввода PIN-кода Администратора или Пользователя.

4.1.1.2 Выбор считывателя

Для выполнения операций непосредственно с устройством прежде всего необходимо выбрать текущий считыватель с подключенным к нему устройством. Выбор считывателя осуществляется из выпадающего списка, содержащего имена считывателей. Считыватели, к которым подключены устройства, отмечены в списке пиктограммой. Для выбора ридера нажмите на соответствующий элемент списка.

4.1.1.3 Получение информации об устройстве

Эта операция доступна в том случае, когда к текущему ридеру подключен идентификатор. Для ее выполнения также не требуется ввод PIN-кода, по-

скольку выдается открытая (не секретная) информация и для ее получения достаточно прав доступа «Гость».

Для получения информации о идентификаторе нужно нажать на кнопку [**Информация...]** в главном окне утилиты.

4.1.1.4 Операция Login

Для выполнения операций разблокирования устройства, изменения PIN-кода и инициализации памяти нужно иметь права доступа Администратора.

После предъявления прав доступа Пользователя становятся доступны только функции изменения PIN-кода Пользователя и символьного имени устройства.

Для установки текущих прав доступа выполняется операция ввода PIN-кода.

После нажатии в главном окне утилиты на кнопку **[Ввести PIN-код]** на экране отображается диалог для ввода PIN-кода:

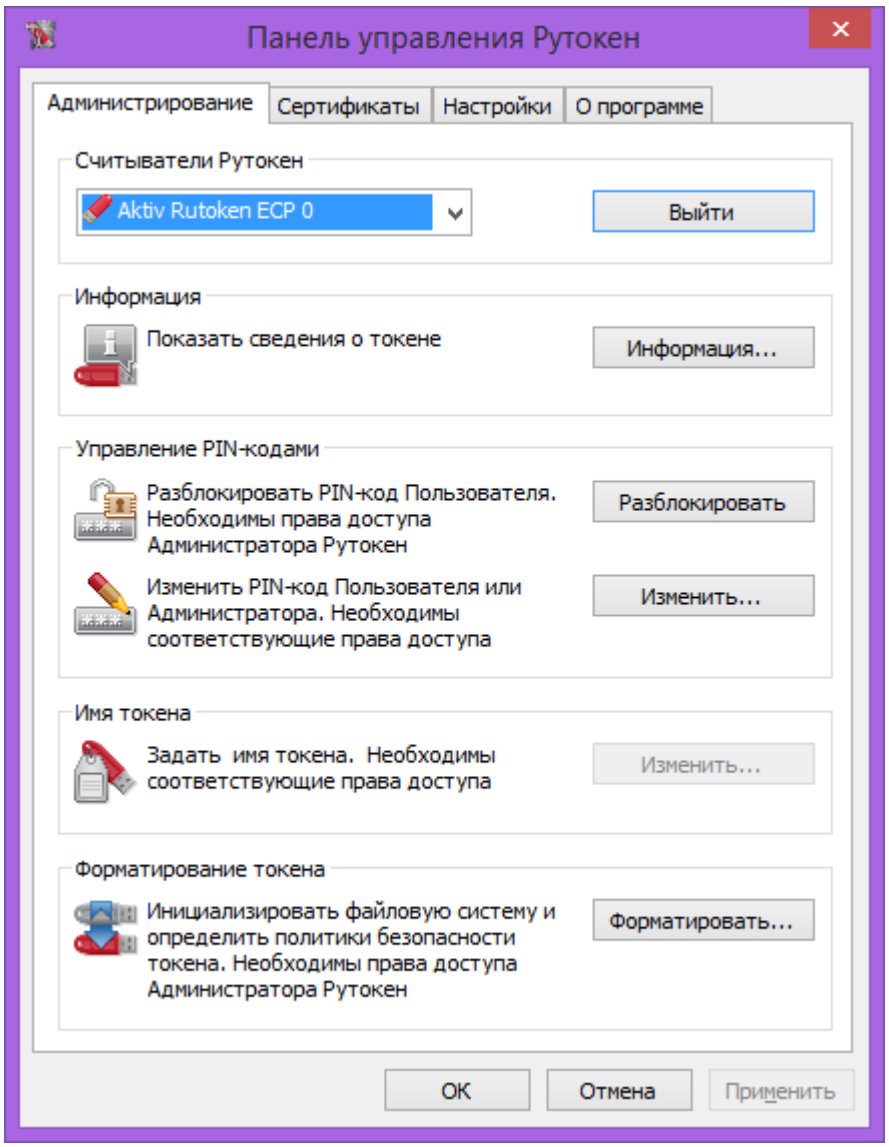
В диалоге требуется выбрать уровень прав доступа из развертывающегося списка (по умолчанию - Администратор) и ввести соответствующий PIN-код.

Набираемый PIN-код отображается в виде символов '*'. Всего может быть предпринято до 10 попыток ввода PIN-кода.

Если выбран уровень прав Администратора, то по исчерпании этого количества попыток PIN-код Администратора блокируется и становится невозможным выполнять любые действия, требующие прав Администратора. Для восстановления полной работоспособности такое устройство следует направлять поставщику (в процессе восстановления устройства все данные на нем будут уничтожены).

В случае ввода правильного PIN-кода активизируются ранее недоступные операции.

После ввода PIN-кода главное окно утилиты будет иметь вид:



4.1.1.5 *Разблокирование PIN-кода Пользователя*

Разблокирование PIN-кода Пользователя ПАК «Рутокен» v. 4 выполняется в тех случаях, когда он был заблокирован после определенного числа последовательных неудачных попыток ввода[*].

Для его разблокирования нужно нажать на кнопку [**Разблокировать]** в главном окне утилиты.

При выполнении этой операции счетчик попыток доступа к соответствующему GCHV-объекту восстанавливается в свое исходное значение, заданное при инициализации устройства.

Для выполнения этой операции необходимо, чтобы текущими были права доступа Администратора.

[*] Число попыток ввода PIN-кодов определяется на этапе инициализации идентификатора и может варьироваться от 3 до 15 для Администратора и от 1 до 15 для Пользователя. Значение по умолчанию – 15.

4.1.1.6 Смена PIN-кода

По умолчанию для PIN-кода Пользователя и PIN-кода Администратора установлены значения '12345678' и '87654321' соответственно.

При работе с ПАК «Рутокен» v. 4» значения PIN-кода по умолчанию необходимо изменить на собственные в целях обеспечения безопасности. Установка новых значений PIN-кодов производится после нажатия на кнопку **[Изменить…]** в главном окне утилиты, в поле Управление **PIN-кодами**:

Диалог установки новых значений PIN состоит из двух групп:

- PIN-код Пользователя – группа предназначена для установки нового PIN-кода Пользователя
- PIN-код Администратора – группа предназначена для установки нового PIN-кода Администратора

Установка PIN-кода Пользователя и Администратора производится по отдельности. Для установки каждого из них необходимо нажать кнопку **[Изменить…]** в соответствующей группе. Максимальная длина PIN-кода – 16 символов, регистр учитывается.

Для смены PIN-кода Администратора необходимо, чтобы текущими были права доступа Администратора.

Владелец устройства, которому разрешено менять PIN-код Пользователя, определяется политикой смены PIN-кода Пользователя, определяемой при инициализации памяти устройства.

4.1.1.7 Изменение символьного имени устройства

Символьное имя устройства служит для облегчения его идентификации.

Для изменения символьного имени устройства требуются права доступа Пользователя. После установки текущих прав доступа и нажатия на кнопку **[Изменить…]** в поле **Управление PIN-кодами** появится диалог, в котором следует указать новое имя устройства.

Максимальная длина символьного имени устройства - 255 байт. Допустимыми являются все отображаемые символы, регистр учитывается.

4.1.1.8 Инициализация памяти устройства

Инициализация памяти предназначена в основном для того, чтобы удалить содержимое памяти устройства – например, при передаче другому владельцу. После выполнения инициализации в памяти устройства содержится только дерево предопределенных папок со служебными файлами, а также GCHV-объекты с PIN-кодами Пользователя и Администратора.

Для запуска инициализации нужно нажать на кнопку **[Форматировать]**:

Перед началом инициализации отображается диалог, состоящий из групп:

- Пользователь – группа предназначена для установки нового PIN-кода Пользователя и числа попыток его ввода (диапазон 1 - 15)
- Администратор – группа предназначена для установки нового PIN-кода Администратора и числа попыток его ввода (диапазон от 3 до 15).

Важная информация

1. Запрещается производить инициализацию памяти устройства в виртуальных машинах типа VMware! Это может привести к порче логической структуры памяти устройства.
2. Категорически запрещается отсоединять идентификатор от USB-порта или извлекать из слота до завершения процесса инициализации! Это может привести к выходу устройства из строя.

После нажатия на кнопку **[Начать]** выводится предупреждение. После подтверждения запускается сам процесс инициализации, прерывать который нельзя.

Для выполнения этой операции необходимо, чтобы текущими были права доступа Администратора.

4.1.1.9 Информация о программе

После выбора вкладки «О программе» появляется окно, в котором показывается версия утилиты.

4.1.2 Вкладка сертификатов Рутокен

Вкладка **[Сертификаты]** предназначена для работы с контейнерами MS CAPI и сертификатами X.509, сохраненными в памяти устройства, и поддерживает следующие операции:

- Просмотр записанных контейнеров MS CAPI и хранящихся в них сертификатов X.509
- Регистрация сертификатов в Личном хранилище сертификатов
- Удаление зарегистрированных сертификатов из Личного хранилища
- Импорт сертификатов из PFX- и CER-файлов в память Rutoken
- Экспорт сертификатов из памяти идентификатора в PFX- и CER-файлы
- Назначение и отмена контейнера по умолчанию
- Удаление контейнеров MS CAPI вместе с их содержимым из памяти устройств ПАК «Рутокен»

Для удобства конечных пользователей, rtCert можно включать в состав любых систем, использующих сертификаты X.509.

4.1.2.1 Главное окно вкладки сертификатов

Перед работой с вкладкой **[Сертификаты]** следует убедиться, что по крайней мере один идентификатор подключен к порту USB. Подсоединить идентификатор можно и после запуска утилиты.

4.1.2.2 Выбор объектов и просмотр их свойств

Для выбора нужного объекта надо щелкнуть правой кнопкой мыши на соответствующей строке списка в окне просмотра. После этого в правом фрейме будут показаны свойства объекта.

Если один из записанных на идентификаторе контейнеров используется системой как контейнер по умолчанию, его имя в списке будет выделено жирным шрифтом.

В контейнерах MS CAPI могут храниться как сертификаты с соответствующими им ключевыми парами, так и отдельные ключевые пары.

При выборе объекта «Ключевая пара» набор показанных свойств будет зависеть от текущих прав доступа, установленных для данного идентификатора:

- Если аутентификация не выполнена (текущие права доступа - Гость), будет показан ограниченный набор свойств ключевой пары
- Если аутентификация выполнена (текущие права доступа - Пользователь), будет показан более полный набор свойств ключевой пары

4.1.2.3 Аутентификация Пользователя

Аутентификация Пользователя необходима для выполнения следующих операций:

- Импорт сертификата из файла в память идентификатора
- Экспорт сертификата из памяти идентификатора в PFX-файл
- Назначение и отмена контейнера по умолчанию
- Удаление контейнера с сертификатами из памяти идентификатора

Для выполнения аутентификации нужно нажать кнопку **[Ввести PIN-код]**.

После завершения операций с идентификатором следует выполнить сброс текущих прав доступа, для чего нужно нажать кнопку.

4.1.2.4 Добавление сертификата в хранилище сертификатов

Эта операция позволяет зарегистрировать выбранный сертификат в Личном хранилище сертификатов данного компьютера. Для выполнения операции пользователю требуется аутентифицироваться.

Для выполнения операции нужно отметить незарегистрированный сертификат, установив флаг в столбце **Зарегистрирован**, затем нажать кнопку

[Применить]. При этом выбранный сертификат будет занесен в память компьютера и зарегистрирован в Личном хранилище.

Зарегистрированный сертификат можно использовать в соответствующем ПО, даже если устройство отсоединено от компьютера.

4.1.2.5 Удаление сертификата из хранилища сертификатов

Эта операция позволяет удалить выбранный сертификат из Личного хранилища сертификатов данного компьютера. При этом из памяти устройства сертификат не удаляется. Для выполнения операции требуется нажать кнопку **[Ввести PIN-код…]** и ввести PIN-код Пользователя, нажать кнопку **[OK]**.

Для выполнения операции нужно снять отметку зарегистрированного сертификат, удалив флаг в столбце **Зарегистрирован**, затем нажать кнопку **[Применить].** При этом выбранный сертификат будет удален из памяти компьютера.

4.1.2.6 Импорт сертификата из файла

На сегодняшний день поддерживается импорт сертификатов из файлов следующих типов:

- Файлы в кодировке DER (CER-файлы)
- Файлы в кодировке Base64 (CER-файлы)
- Файлы обмена личной информацией (PFX-файлы)
    - Файлы формата *.p12.

Для выполнения операции импорта открыть вкладку, нажать кнопку [**Ввести PIN-код…]**

При нажатии кнопки **[Импортировать]** появляется диалоговое окно.

Импорт сертификата

При импорте из CER-файла следует учитывать, что в таком файле может храниться только сам сертификат без соответствующей ему ключевой пары. Импорт из CER-файла возможен при выполнении двух условий:

- Импорт производится в контейнер MS CAPI, уже существующий в памяти устройства
- В этом контейнере уже хранится, как минимум, ключевая пара, соответствующая импортируемому сертификату (либо сам сертификат с ключевой парой)

Таким образом, на сегодняшний день импорт из CER-файла практически применим только для обновления или восстановления содержимого контейнера, по каким-либо причинам испорченного в процессе работы.

Для импорта необходимо в открывшемся окне указать имя файла с импортируемым сертификатом, указать, является ли он файлом обмена личной информацией или сертификатом формата X.509, нажать кнопку **[Открыть]**.

В диалоговом окне ввести пароль для доступа к файлу обмена личной информацией.

Имя контейнера можно задать вручную, либо сгенерировать, нажав кнопку **[Уникальное имя]**.

Нажать **[Импортировать]**.

Импортированный сертификат будет виден в списке.

4.1.2.7 Назначение сертификата

Для назначения контейнера соответствующей ключевой паре требуются права Пользователя.

Для назначения сертификата ключевой паре следует выделить его кнопкой мыши, нажать кнопку [**Назначить сертификат]**, в открывшемся окне указать путь к сертификату и нажать кнопку **[Открыть]**.

Сертификат на устройстве будет обновлен.

4.1.2.8 Назначение контейнера по умолчанию

Понятие контейнера по умолчанию весьма часто используется в ОС Windows. Так, для осуществления Logon в домене Windows используется сертификат, хранящийся в контейнере по умолчанию.

Для того чтобы назначить контейнер по умолчанию нужно отметить контейнер в окне просмотра и нажать кнопку **[По умолчанию]**. По окончании операции контейнер получит признак «по умолчанию» и будет помечен в списке жирным шрифтом.

Если в памяти устройства уже существовал контейнер по умолчанию, новый контейнер станет контейнером по умолчанию вместо него (т. е. может существовать только один контейнер по умолчанию).

Для выполнения данной операции требуются права доступа Пользователя.

Отмена контейнера по умолчанию

Выписанный сертификационным центром сертификат с признаком Smartcard Logon или Smartcard User чаще всего записывается в контейнер по умолчанию. Если же в памяти устройства уже существует контейнер по умолчанию, он может быть физически уничтожен (т. е. перезаписан новым контейнером).

Чтобы избежать этого и сохранить сертификат из контейнера по умолчанию, утилита rtCert предоставляет возможность отменить регистрацию этого контейнера как контейнера по умолчанию.

Для выполнения операции нужно отметить контейнер по умолчанию в окне просмотра rtCert (контейнер по умолчанию выделен в списке жирным шрифтом) и нажать кнопку **[По умолчанию]** в нижней части панели. По окончании операции в памяти идентификатора не будет контейнера по умолчанию, и теперь можно безопасно выписывать новый сертификат.

Для выполнения операции требуются права доступа Пользователя.

4.1.2.9 Удаление контейнера

Эта операция позволяет удалить из памяти устройства контейнер MS CAPI вместе со всем его содержимым.

Для выполнения операции требуются права доступа Пользователя.

Для удаления контейнера нужно выделить контейнер, нажать кнопку **[Удалить]**. После соответствующего предупреждения контейнер со всем содержимым будет физически удален из памяти устройства.

4.1.3 Вкладка «Настройки» Панели управления Рутокен

4.1.3.1 Считыватели Рутокен

Для увеличения количества считывателей Рутокен требуется установить число, затем нажать кнопку **[Применить]**.

4.1.3.2 Настройки PIN-кода

Окно Настройки PIN-кода позволяют

- Кэшировать PIN-код.
- Предлагать сменить PIN-код при каждом использовании PIN-кода по умолчанию.
- Кодировать PIN-код в UTF-8.

Для установки каждой настройки необходимо нажать кнопку **[Настройка…]**, отметить её флагом, затем нажать кнопку **[Применить]**.

4.1.3.3 Настройки криптопровайдера по умолчанию

Для настройки криптопровайдера необходимо в окне Настройки криптопровайдера по умолчанию нажать кнопку **[Настройка]**, выбрать для каждого идентификатора криптопровайдер по умолчанию, а также выбрать криптопровайдер для генерации ключей идентификатора Рутокен ЭЦП.

После выбора криптопровайдеров нажать кнопку **[Применить]**.

4.2 Использование на ОС семейства Linux

Утилита rtAdmin предназначена для автоматизации процедур форматирования и администрирования устройств Рутокен: смены метки идентификатора, PIN-кодов и их параметров, управления разделами Flash-памяти.

При работе с утилитой рекомендуется не подключать более одного устройства.

4.2.1 Параметры rtAdmin

№	Описание команды	Параметр командной строки	Значение по умолчанию
1	Форматирование идентификатора	-f	-
2	Текущий PIN-код администратора	-o [PIN-код (≤ 32)]	87654321 Значение по умолчанию используется только при форматировании без указания параметра -o
3	Текущий PIN-код пользователя	-c [PIN-код (≤ 32)]	12345678 Значение по умолчанию используется только при форматировании без указания параметра -c
4	Устанавливаемый PIN-код администратора	-a [PIN-код (≤ 32)]	87654321 Значение по умолчанию используется только при форматировании без указания параметра -a
5	Устанавливаемый PIN-код пользователя	-u [PIN-код (≤ 32)]	12345678 Значение по умолчанию используется только при форматировании без указания параметра -u
6	Устанавливаемый PIN2-код (для Рутокен PINPad. Устанавливается на экране устройства)	-t	-
7	Генерация PIN-кода администратора (используется при форматировании)	-G [длина PIN-кода (8-32)]	-
8	Генерация PIN-кода пользовате-	-g [длина PIN-кода (8-	-

	ля (используется при форматировании)	32)]	
9	Загрузка значений пар PIN-кодов из файла	-b [имя файла]	-
10	Политика смены PIN-кода пользователя	-p [кто может менять PIN-код: 1 – администратор, 2 – пользователь, 3 – пользователь и администратор]	2
11	Минимальная длина PIN-кода администратора	-M [длина PIN-кода (6-31 для Рутокен ЭЦП и Рутокен Lite, 1 для Рутокен S)]	6
12	Минимальная длина PIN-кода пользователя	-m [длина PIN-кода (6-31 для Рутокен ЭЦП и Рутокен Lite, 1 для Рутокен S)]	6
13	Максимальное количество попыток ввода PIN-кода администратора	-R [число попыток (3-10)]	10
14	Максимальное количество попыток ввода PIN-кода пользователя	-r [число попыток (1-10)]	10
15	Метка идентификатора в кодировке Windows-1251	-L [метка идентификатора]	-
16	Метка идентификатора в кодировке UTF-8	-D [метка идентификатора]	-
17	Конвертация в UTF-8 (флаг для параметров, связанных с PIN-кодами)	-U	По умолчанию PIN-коды не конвертируются в UTF-8
18	Ограничение количества выполняемых итераций до одной	-q	-
19	Используемая библиотека PKCS#11	-z [путь к библиотеке]	rtPKCS11.dll
20	Путь к конфигурационному файлу	-n [путь к файлу]	-
21	Протоколирование	-l [путь к файлу лога]	Путь: каталог, в котором лежит утилита Имя файла: rtadmin.exe.log

Параметры для управления флеш-памятью (Рутокен Flash)

22	Разбиение Flash-памяти на разделы (форматирование) **Внимание!** Форматирование удалит всю информацию с Flash-памяти. Сделайте копию важной информации - после форматирования ее бу-	-F [идентификатор раздела (1-8)] [размер в Мб] [владелец: a - администратор, u - пользователь, l3-l9 - локальный	1 весь объем (1DDC сейчас) a rw

	дет невозможно восстановить.	пользователь] [права доступа: ro, rw, hi, cd]	
23	Изменение прав доступа	-C [идентификатор раздела (1-8)] [новые права доступа: ro, rw, hi, cd] [долговременность: p - постоянное изменение, t - временное]	не определено не определено t
24	Получение информации о размере Flash-памяти и атрибутах разделов	-i [a - атрибуты всех разделов] [1-8 - атрибуты конкретного раздела] [sz - объем памяти] Формат ответа – аналогично п.21 Разбиение Flash-памяти на разделы (форматирование): [идентификатор раздела (1-8)] [размер в Мб] [владелец: a - администратор, u - пользователь, l3-l9 - локальный пользователь] [права доступа: ro, rw, hi, cd]	sz

Параметры для управления локальными пользователями

25	Устанавливаемый PIN-код локального пользователя	-B [идентификатор локального пользователя (l3-l9)] [PIN-код]	-
26	Текущий PIN-код пользователя	-O [идентификатор локального пользователя (l3-l9)] [PIN-код]	Если PIN-код для данного пользователя не определен, текущий PIN-код указывать не требуется

При необходимости параметры командной строки могут быть переданы с помощью конфигурационного файла.

В случае отсутствия заданных PIN-кодов при форматировании устанавливаются PIN-коды по умолчанию.

Утилита является циклической и после выполнения заданных действий на подключенном идентификаторе ожидает подключения следующего.

5. АВАРИЙНЫЕ СИТУАЦИИ

№ п/п	Нештатная ситуация	Действия при нештатной ситуации
1.	Выход электронного идентификатора из строя	Необходимо сообщить администратору безопасности о выходе из строя аппаратного модуля и обеспечить его доставку администратору безопасности для выяснения причин выхода из строя.
2.	Отказы в работе программных средств вследствие случайного или умышленного их повреждения.	При отказах в работе программных средств, в следствии случайного или умышленного их повреждения, лицо, ответственное за безопасность функционирования программных и аппаратных средств, обязано произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы программных средств в установленном порядке.
3.	Ошибка: Неправильный пин-код	Нужно повторить ввод пин-кода, однако после третей неудачной попытки пин-код блокируется